ASSEMBLÉE NATIONALE

13ème législature

informatique

Question écrite n° 53082

Texte de la question

M. Thierry Lazaro attire l'attention de M. le secrétaire d'État chargé de l'outre-mer sur la multiplication des virus informatiques dont la conception relève de plus en plus du domaine de la cybercriminalité. De nombreux pays se sont déjà penchés sur les conséquences dramatiques qui pourraient résulter d'une attaque menée par des cyberterroristes contre les systèmes informatiques de leurs administrations. Aussi, il lui demande de bien vouloir lui faire part des réflexions menées au sein de son ministère ainsi que des services et administrations qui en dépendent, et de le rassurer sur l'efficacité des parades mises en oeuvre en la matière, de façon à éviter que les systèmes informatiques concernés ne puissent être détruits, ou que des données confidentielles ne puissent être transmises à ces cyberterroristes.

Texte de la réponse

Pour renforcer la cohérence et la capacité propre des moyens de l'État en matière de sécurité des systèmes d'information (SSI), le Livre blanc sur la défense et la sécurité nationale a proposé la création d'une Agence nationale de la sécurité des systèmes d'information (ANSSI), relevant du Premier ministre par l'intermédiaire du secrétaire général pour la défense et la sécurité nationale (SGDSN). Cette agence, créée par le décret 2009-834 du 7 juillet 2009, a notamment pour missions de détecter les attaques informatiques des réseaux les plus sensibles de l'administration et de réagir au plus tôt, grâce à un centre opérationnel renforcé de cyberdéfense, actif 24 h/24 h. Pour décliner sur l'ensemble du territoire national les mesures prises afin d'améliorer la sécurité des systèmes d'information, le Livre blanc a également prévu de doter chaque zone de défense d'un observatoire zonal de la sécurité des systèmes d'information (OZSSI), placé sous l'autorité du préfet de zone. Ouverts à l'ensemble des administrations, tous les observatoires ont été installés en 2009. Concernant plus particulièrement le ministère de l'intérieur, de l'outre-mer et des collectivités territoriales, sa responsabilité s'exerce à plusieurs niveaux. Tout d'abord, la protection des réseaux internes est assurée par le haut fonctionnaire de défense (HFD), responsable de la politique des systèmes d'information du ministère, qui dispose pour cela de la direction de la planification de sécurité nationale (DPSN). Cette direction a développé en 2009 un plan d'action cyberdéfense, mis en oeuvre par le Centre national de gestion et d'Expertise de la SSI (CNGESSI), qui renforce la protection des systèmes et des données confidentielles. Ce plan, couplé avec celui de l'ANSSI, développe la veille et la détection des attaques par une analyse poussée des signaux précurseurs issus du réseau des 350 correspondants locaux (responsables SSI) et par l'exploitation des signaux quotidiens générés par les systèmes techniques des infrastructures réseau et informatique. Ensuite, le ministère de l'intérieur exerce également un rôle de lutte contre la cybercriminalité pour le grand public et les entreprises. Trois directions sont en charge de ce dispositif. La direction générale de la police nationale (DGPN) avec l'Office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication (OCLCTIC), qui traite sur le plan judiciaire les infractions spécifiques à ce type de criminalité. La direction centrale du renseignement intérieur (DCRI) qui protège les intérêts de la nation sur le territoire national et suit l'activité des entreprises nationales spécialisées dans le domaine des Technologies de l'information et de la communication (TIC). La direction générale de la gendarmerie nationale (DGGN) dont le dispositif intégré

s'articule autour de trois pôles opérationnels et techniques : l'institut de recherche criminelle de la gendarmerie nationale (IRCGN) et le service technique de recherches judiciaires et de documentation (STRJD) au plan national ; le réseau des 190 enquêteurs en technologies numériques (NTECH) dans les sections de recherches et brigades départementales de renseignements et d'investigations judiciaires. Enfin, deux mesures dans le domaine de la cybercriminalité ont été intégrées dans le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) : le blocage des sites proposant des images de mineurs à caractère pornographique et la création d'une nouvelle incrimination relative à l'utilisation frauduleuse de données à caractère personnel.

Données clés

Auteur : M. Thierry Lazaro
Circonscription : Nord (6e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 53082
Rubrique : Ministères et secrétariats d'état
Ministère interrogé : Outre-mer
Ministère attributaire : Intérieur, outre-mer et collectivités territoriales

Date(s) clée(s)

Question publiée le : 23 juin 2009, page 6064
Réponse publiée le : 11 mai 2010, page 5334